Abstract of the Disclosure

METHOD AND APPARATUS FOR UNIQUELY AND AUTHORITATIVELY IDENTIFYING TANGIBLE OBJECTS

A smart chip protection system contains a unique public/private identity key pair and uses a separate public/private signature key pair. The identity private key is stored in permanent, secure storage such that it can not be read outside the chip. An issuing entity generates a descriptor containing the identity public key, attribute data, and a digital signature. The digital signature is generated by enciphering a derivation of the identity public key and the attribute data with the signature private key known only to the issuer. The authenticity of the descriptor data is verified by decrypting the signature with the signature public key using a known algorithm, and comparing the result to the derivation of the descriptor data. The identity of the object can be verified requesting the smart chip ro perform an encryption/decryption operation using its identity private key, and performing the complement using the public key.